基于特征值的黑盒子意义下的特殊门限秘密共享方案 *

张艳硕 [1,2]，李文敬 [1,2]，史国振 [1]，蒋　华 [1]，陈　雷 [1]，杨　涛 [2]

(1. 北京电子科技学院，北京 100070; 2. 公安部第三研究所，上海 201204)

摘　要：基于 Shamir(n，t)秘密共享方案，提出一个新的门限秘密共享方案。利用 n 阶矩阵的特征方程具有重根的特点，实现了不同集合中参与者的秘密共享。同一参与集合所对应的次主密钥是相同的，即特征值是相同的，将同一个特征值所对应的不同特征向量作为子密钥，分发给同一参与集合的参与成员。而且利用黑盒子，同一集合内部成员可以验证自己手中的子密钥的真实性，从而达到了防欺诈的目的。分析结果表明，本方案是安全的理想秘密共享方案。

关键词：Shamir(n,t)秘密共享；对称矩阵；特征值；特征向量；黑盒子

中图分类号：TP309　　doi: 10.3969/j.issn.1001-3695.2018.01.0167

Special threshold secret sharing scheme in sense of black box based on eigenvalue

Zhang Yanshuo[1, 2], Li Wenjing[1, 2], Shi Guozhen[1], Jiang Hua[1], Chen Lei[1], Yang Tao[2]

(1. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*; 2. *The Third Research Institute of Ministry of Public Security*, *Shanghai* 201204, *China*)

Abstract: This paper proposed a new threshold secret sharing scheme based on the Shamir(n, t) threshold secret sharing scheme. Used the characteristic that the characteristic equation of the n-th order matrix has multiple roots, realized the secret sharing of participants in different sets. The secondary master key corresponding to the same participation set is the same, that is, the eigenvalue are the same. The algorithm firstly used the feature vector corresponding to the same eigenvalue as a subkey , then it distributed the subkey to the participating members of the same participating set. what's more, the members of the same collection could use the black box to verify the authenticity of the sub-keys in their own hands so as to achieve the purpose of fraud prevention. The analysis result shows that this scheme is safe and ideal .

Key words: Shamir(n,t) secret sharing; symmetric matrix; eigenvalues; feature vector; black box key

0　引言

秘密共享方案为解决信息安全和密钥管理问题提供了一个崭新的思路，在重要信息和秘密数据的安全存储、传输及合法利用中起着非常关键的作用。自 Shamir[1]和 Blakley[2]在 1979 年分别提出了门限秘密共享体制以来，有关秘密共享体制的研究受到了广泛的研究，并取得了丰硕的成果。

Ito 等人 [3]中描述了秘密共享的一般方法，给出了实现任意单调访问结构的秘密共享方案的相关技术。Laih 等人[4]提出了动态秘密共享的概念：主秘密可以随意更新而参与者拥有的子秘密值可以保持不变。Zarepour-Ahmadabadi 等人[6]提出了一种新颖高效的算法以解决动态密钥通信量成本高的问题。Traverso 等人[5]提出了基于 Birkhoff 插值的第一个动态和可验证的分层秘密共享方案。Yang 等人[7]提出了一个加权超椭圆秘密共享方案。Binu[8]等人提出了一个具有单调广义访问结构的秘密共享方案，利用 Shamir 方案和椭圆曲线配对的方法使得该方案具有可验证性。Jarecki 等人[9]提出了第一轮最优 PPSS 方案。Pilaram 等人[10]根据 Ajtai 的单向函数构造，提出了一个基于格的门限多级秘密共享（MSSS）方案。Sarkar和 Wang 等人[11,12]基于双线性对（BLP）映射分别提出了秘密共享方案。

本文在 Shamir 门限方案的基础上，利用 n 阶对称矩阵的特征方程具有重根的特点，提出了一个基于特征值的门限秘密共享方案的设计新方法。同时，本方案设计了一个“黑盒子”，并利用“黑盒子”实现子秘密生成和主密钥恢复的功能。经过分析证明，该方案是完善理想的，且在理论上是不可攻破的。

收稿日期：2018-01-22；**修回日期：**2018-04-08　**基金项目：**国家重点研发计划基金资助项目（2017YFB0801803）；中国民航信息技术科研基地资助项目（CAAC-ITRB-201705）

作者简介：张艳硕（1979-），男，陕西宝鸡人，博士，主要研究方向为密码理论及其应用；李文敬（1992-），女，山东济宁人，硕士研究生，主要研究方向为信息安全（2654019946@qq.com）；史国振（1974-），男，河南济源人，博士，主要研究方向为网络与系统安全、嵌入式系统；蒋华（1962-），山西大同人，教授，博士，主要研究方向为通信与信息安全；陈雷（1992-），男，河北邯郸人，硕士研究生，主要研究方向为信息安全；杨涛（1977-），男，博士，副研究员，主要研究方向为信息安全.

1 预备知识

为了方案描述方便，先介绍一下用到的基础知识。

1.1 方阵的特征值和特征向量

定义 1[13] 设 A 是 n 阶矩阵，如果数 λ 和 n 维非零列向量 p 使关系式：

$$p^{-1}Ap=\lambda \tag{1}$$

成立，那么，这样的数 λ 称为矩阵 A 的特征值，非零向量 p 称为 A 的对应于特征值 λ 的特征向量。式（1）也可写成

$$(A-\lambda E)p=0 \tag{2}$$

这是 n 个未知数 n 个方程的齐次线性方程组。

1.2 对称矩阵的性质

定理 1 设 A 为 n 阶对称矩阵，则必有正交矩阵 P，使

$$P^{-1}AP=\Lambda=\begin{pmatrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{pmatrix} \tag{3}$$

其中：Λ 是以 A 的 n 个特征值 λ_i（$i=1,2,\cdots,n$）为对角元的对角矩阵。

推论 1 设 A 为 n 阶对称矩阵，λ 是 A 的特征方程的 k 重根，从而对应特征值 λ 恰有 k 个线性无关的特征向量。

1.3 黑盒子

1.3.1 黑盒子的定义

所谓“黑盒子”，是指从用户的角度来看一个器件或产品时，并不关心其内部构造和原理，而只关心它的功能及如何使用这些功能[14]。

本文基于上述定义，给出本方案中的定义：

定义 2 黑盒子的内部结构只有其设计者知道，除此之外无人知晓。子秘密生成阶段，分发者输入主密钥 K，参与者输入集合的个数 t 和每个集合的人数 n_i，黑盒子生成 n（$\sum_{i=1}^{t}n_i=n$）个特征向量 p_{ij}（$1\le i\le t$，$1\le j\le n_i$），并将该特征向量 p_{ij} 作为子秘密分发给各集合的参与者。主密钥恢复阶段，各集合的参与者输入子密钥 p_{ij}，若输入的子秘密是真实的，则得到所对应的特征值 λ_i，从而恢复主密钥 K，否则，不能恢复主密钥 K。

1.3.2 黑盒子的原理

a）子秘密生成阶段，根据式（3）设计的，即

$$P^{-1}\Lambda P=A$$

其中：P 为生成的随机对称矩阵；Λ 是以特征值 λ_i 为对角元素的对角矩阵，所求的子秘密 p_{ij} 是矩阵 A 的特征向量。

b）主密钥恢复阶段，根据式（1）设计的，即

$$p_{ij}^{-1}Ap_{ij}=\lambda_i$$

其中：矩阵 A 是子秘密生成阶段所生成的矩阵，存储在黑盒子中。当参与者输入正确的子秘密 p_{ij} 时，黑盒子输出该子秘密对应的特征值 λ_i。如果输入错误的子秘密 p_{ij}，则无法得到特征值。

1.4 密码学知识

定义 3 秘密分发者。是指把子秘密分发给 n 个共享参与者的人或设备。他的任务还包括向公告牌上公布相应的辅助信息。

定义 4 秘密参与者。是指拥有一份子秘密，并且可以通过与足够多的其他参与者的合作，得到共享秘密的人或者设备。

定义 5 公告栏。秘密分发者发布辅助信息的媒介，如 web 网站等。公告牌只有秘密分发者可写，而参与者只有阅读权限。

2 Shamir 门限方案

1979 年 Shamir[1]基于多项式的 Lagrange 插值公式提出了一个（n，t）门限方案，称为 Shamir 门限方案或 Lagrange 插值法。Shamir 门限方案的详细介绍如下。

a）参数选取

设共享秘密 K，选择一个素数 $p\in Z_p$（$p>t$），有 n 个参与者，要求重构该共享秘密 K 至少 t 个人。

b）秘密分割

首先，随机地选定 $t-1$ 个互不相同的数，记为 a_1，a_2，$\cdots$ a_{t-1} $\in Z_p$，得到多项式：

$$s(x)=K+a_1x+\cdots+a_{t-1}x^{t-1}(\bmod p) \tag{4}$$

该多项式满足 $s(0)\equiv K \bmod p$。

其次，选定 n 个不同的整数 $x_1,x_2,\cdots,x_n$ $\in Z_p$（如选择 1,2,…，n），对于每个整数分别计算数对（x_i，y_i），其中 $y_i\equiv s(x_i) \bmod p$。

最后，将 n 个数对（x_i，y_i），$i=1,2,\cdots,n$ 分别秘密传送给 n 个成员，多项式 $s(x)$ 则是保密的，可以销毁。

c）秘密恢复

假设 t 个人一起准备恢复秘密 K，不妨设他们的数对为（x_1，y_1），（x_2，y_2），…，（x_t，y_t）。

首先，t 个人计算多项式 $f(x)$：

$$f(x)\equiv\sum_{k=1}^{t}y_k\prod_{\substack{j=1\\ j\ne k}}^{t}\frac{x-x_j}{x_k-x_j}(\bmod p) \tag{5}$$

其次，取多项式 $f(x)$ 的常数项 $f(0)$，即为所求的秘密 K。

3 基于特征值的黑盒子意义下的特殊门限秘密共享方案

3.1 方案定义

在给出本门限方案以前，先给出一个例子。三家银行 B_1、B_2 和 B_3 共同管理一项基金，基金的使用需要经过三家银行的执行董事都同意才能使用该基金。其中，银行 B_1 有 3 个执行董事，银行 B_2 有 4 个执行董事，银行 B_3 有 3 个执行董事。在这个例子中，每家银行均只需派出任意一位执行董事，即可决定基金的使用状况，则一共有 $3\times4\times3=36$ 种决定方式。由此，本文定义了一种新的 $(n_1+n_2+\cdots+n_t,1+1+\cdots+1)$ 门限方案。

定义 6 设 B_1，B_2,…，B_t 是 t 个参与者的集合，$B_1\cap B_2\cdots\cap B_t=\Phi$，$|B_1|=n_1$，$|B_2|=n_2$，…，$|B_t|=n_t$（$n_1+n_2+\cdots+n_t=n$），集合 B_1 中的 n_1 个参与者中每人分得一个秘密数对（x_1，p_{1j}）（$1\le j\le n_1$），B_2 中的 n_2 个秘密参与者中每人分得一个秘密数对（x_2，p_{2j}）（$1\le j\le n_2$），…，B_t 中的 n_t 个秘密参与者中每人

分得一个秘密数对（ x_t ， p_{tj} ）（ $1 \le j \le n_t$ ）。每个集合至少都出一个人则可以计算出密钥 K ，缺少任何 1 个集合的秘密参与成员都不能计算出密钥 K 。

3.2 方案实施

提出的新方案包括参数假设、秘密分发、秘密恢复三个部分，详细描述如下。

3.2.1 参数假设

设秘密参与者一共有 $n_1 + n_2 + \cdots + n_t = n$ 个人，（参与者集合 B_1，B_2,⋯，B_t，分别各有 $n_1, n_2, \cdots, n_t$ 个人），设 p （ $p > t$ ）是素数。秘密分发者随机地选定 $t-1$ 个数，记为 a_1， a_2， ⋯， $a_{t-1} \in Z_p$，得到多项式 $s(x) \equiv K + a_1 x + \cdots + a_{t-1} x^{t-1} (\mathrm{mod}\ p)$ 。

其中，共享秘密主密钥是 K 。

3.2.2 秘密分发

首先，秘密分发者选择 t 个非零的、互不相同的元素 $x_1, x_2, \cdots, x_t \in Z_p$，分别计算 $\lambda_i = s(x_i)$ （ $i = 1, 2, \cdots, t$ ），得到 n 阶对角矩阵 Λ 。

$$\Lambda = \begin{pmatrix} \lambda_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \lambda_1 & & & & & & \\ & & & \lambda_2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & \lambda_2 & & & \\ & & & & & & \ddots & & \\ & & & & & & & \lambda_t & \\ & & & & & & & & \ddots \\ & & & & & & & & & \lambda_t \end{pmatrix} \begin{matrix} \}\lambda_1 \\ \\ \}\lambda_2 \\ \\ \}\lambda_t \end{matrix}$$

其中：$\lambda_1, \lambda_2, \cdots, \lambda_t$ 是特征方程式（1）对应的特征根，并且 λ_1 有 n_1 个， λ_2 有 n_2 个， ⋯， λ_t 有 n_t 个。

其次，秘密分发者随机生成一个足够大的 n 阶对称矩阵 P ，进而得到矩阵 A ：

$$A = P^{-1} \Lambda P \tag{6}$$

由线性代数知识可知，矩阵 Λ 和矩阵 A 具有相同的特征值。又由推论 1 可知，每个特征根 λ_i $(i = 1, 2, \cdots, t)$ 对应 n_i 个线性无关的特征向量。此时将 λ_i 作为次主密钥。其中， λ_1 对应的特征向量为 $(p_{11}, p_{12}, \cdots, p_{1n_1})$， λ_2 对应的特征向量为 $(p_{21}, p_{22}, \cdots, p_{2n_2})$， ⋯， λ_t 对应的特征向量为 $(p_{t1}, p_{t2}, \cdots, p_{tn_t})$ 。秘密分发者将（ x_i ， p_{ij} ）（ $1 \le i \le t$ ，$1 \le j \le n_i$ ）作为子密钥分发给不同参与集合的参与者。其中 x_i 是公开的， p_{ij} 是属于 λ_i 的私有子密钥。

3.2.3 秘密恢复

由于门限的特殊性，要求恢复秘密的参与者的个数达到要求，即不少于门限值 t ，也就是说每个参与者集合必须至少出一个人，且不失一般性。假设 B_1 中恢复秘密的 1 个参与者的子密钥是（ x_1 ， p_{11} ），B_2 中恢复秘密的 1 个参与者的子密钥是（ x_2 ， p_{21} ），⋯，B_t 中恢复秘密的 1 个参与者的子密钥是（ x_t ， p_{t1} ）。

首先，每个参与者向黑盒中输入自己的子秘密 p_{ij}，得到 λ_i 。

然后，将（ x_1 ， λ_1 ）、（ x_2 ， λ_2 ）、⋯⋯（ x_t ， λ_t ）代入方程 $s(x) = a_0 + a_1 x + a_2 x + \cdots + a_{t-1} x^{t-1}$ 。得到方程组：

$$\begin{cases} s(x_1) = a_0 + a_1 \bullet x_1 + \cdots + a_{t-1} \bullet x_1^{t-1} = \lambda_1 \\ s(x_2) = a_0 + a_1 \bullet x_2 + \cdots + a_{t-1} \bullet x_2^{t-1} = \lambda_2 \\ \cdots \\ s(x_t) = a_0 + a_1 \bullet x_t + \cdots + a_{t-1} \bullet x_t^{t-1} = \lambda_t \end{cases} \tag{6}$$

由于 $s(x)$ 是 $t-1$ 次曲线，所以如果知道了 t 个点，曲线就可以按拉格朗日差值公式表达出来： $f(x) = \sum_{i=1}^{s} \lambda_i \prod_{\substack{j=1 \\ j \ne i}}^{s} \frac{x - x_i}{x_i - x_j}$ 。而 $f(x)$ 在 $x = 0$ 点的值就是共享密钥： $K = f(0)$ 。

3.3 黑盒子的实现

3.3.1 功能介绍

黑盒子是本方案的核心。为了更好地理解本方案，将详细介绍黑盒子的功能，其中黑盒子的功能结构见图 1。

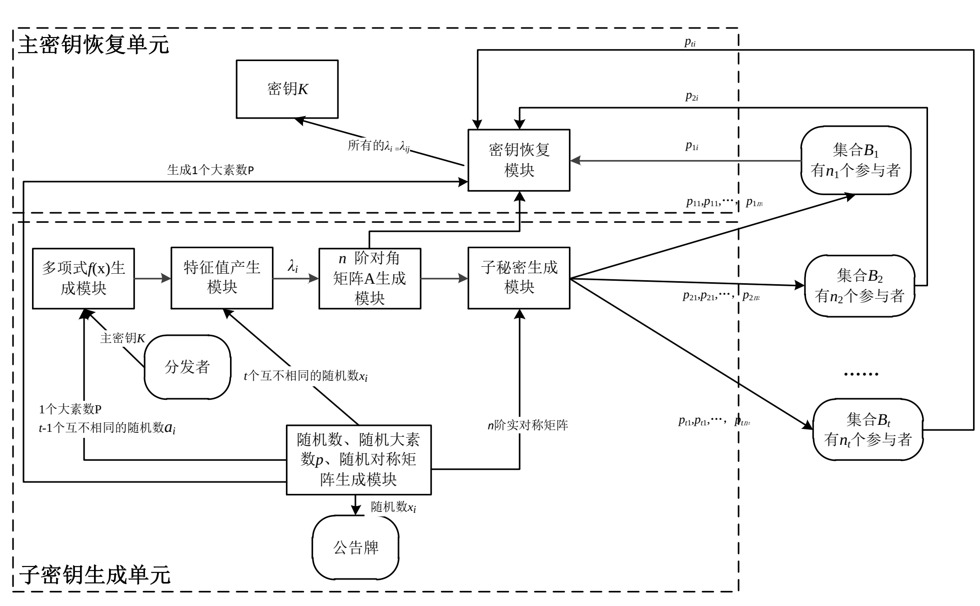


图 1 黑盒子功能结构

黑盒子包括子密钥生成单元和主密钥恢复单元。子密钥生成单元包括随机数、随机大素数、随机对称矩阵生成模块、多项式生成模块、特征值产生模块、n 阶对角矩阵 Λ 生成模块和子秘密生成模块。其中，子密钥生成单元只有分发者有权利输入数据。主密钥生成单元相对简单，只包括密钥恢复模块。

具体功能介绍如下：

a)模块一——随机数、随机大素数、随机对称矩阵生成模块。根据指令可以生成随机数、随机大素数、随机对称矩阵。

b)模块二——多项式生成模块。根据生成个随机数、大素数和主密钥，生成多项式 $f(x)$。

c)模块三——特征值产生模块。根据生成的随机数 x_i，得到 x_i 所对应的特征值 λ_i。

d)模块四—— n 阶对角矩阵 Λ 生成模块。根据各集合中的人数 n_i 和 λ_i，可以生成 n 阶实对称矩阵。

e)模块五——子秘密生成模块。根据生成的生对称矩阵 P 和对角矩阵 Λ，得到矩阵 $A=P^{-1}\Lambda P$，从而得到 n 个特征向量 p_{ij}，作为子密钥分发给各集合参与者。

f)模块六——密钥 K 恢复模块。各集合的参与者将自己得到的子密钥输入到黑盒子去，若输入正确的子密钥，则得到次主密钥，即特征值，从而得到主密钥；否则，不能恢复主密钥。

3.3.2 功能实现

1）子密钥分发过程

a)生成多项式 $f(x)$。

根据参与者集合的个数 t、参与者总人数 n，模块一生成一个随机大素数 p、$t-1$ 个随机数 a_i（$i=1,2,\cdots,t-1$），并送到模块二中。同时，分发者将主密钥 K 也输入模块二中，和上述数据生成多项式 $f(x)$，并将其送到模块三中。

b)生成特征值 λ_i。

将模块一生成 t 个随机数 x_i（$i=1,2,\cdots,t$）发送到模块三中，得到 t 个特征值 λ_i。

c)生成对角矩阵 Λ。

模块四根据输入集合的合数 t、每个集合的人数 n_i 和所对应的特征值 λ_i，生成 n 阶对角矩阵 Λ。

d)生成子秘密。

模块五利用模块一生成的对称矩阵 P 和模块四生成的对角矩阵 Λ，得到矩阵 $A=P^{-1}\Lambda P$，从而得到 n 个特征向量 p_{ij}，作为子密钥分发给各参与者。

2）主密钥恢复过程

各集合的参与者将自己得到的子密钥 p_{ij} 输入到黑盒子去，若所有的参与者输入的子密钥都是正确，则得到主从密钥，从而得到主密钥；否则，不能恢复主密钥。

3.3.3 黑盒子主要功能程序

本黑盒子的设计，是以 MATLAB 为语言环境的，主要的功能程序为：

a)生成大素数

```
psl=[10,20];
asl=primes(psl(1));
bsl=primes(psl(2));
csl=setxor(asl,bsl);
msl=round(1+(numel(csl)-1)*rand());
p=csl(msl);
```

b)生成随机数

```
function d=randnorepeat(m,n)
p=randperm(n);
d=p(1:m);
end
```

c)生成随机对称矩阵

```
m=diag(Ei);
a=rand(n,n);
b=tril(a,-1)+triu(a',0)
```

d)生成多项式 $f(x)$ 和特征值 λ_i

```
Ei=[ ] ;
for j=1:t
      fx=K;
      fxy=K;
       xi=xii(1,j)
       fprintf('%d',xi)
       ni=input('所对应的集合的人数:') ;
     for i=1:t-1
       fx=fx+a(1,i)*(x^(i));
       fxy=fxy+a(1,i)*(xi^(i));
     end
     for k=1:ni
      Ei=[Ei mod(fxy,p)];
     end
 end
```

e)生成矩阵 A

```
dm=b^-1*m*b
```

f)生成子秘密

```
[V,D]=eig(dm)
for l=1:n
   fprintf('得到子秘密')
   V(:,l)
end
```

g)恢复主密钥

```
fprintf('请输入得到子秘密')
pz= input('要输入的数 pz:')
la=pz^-1*m*pz
```

4 安全性

4.1 正确性[16]

本方案的正确性，分两步证明：

a)证明 t 个集合构造出来的多项式满足 $s(x_i)=f(x_i)=\lambda_i$，$i=1,2,\cdots,t$。

令 $l_k(x)=\prod_{\substack{j=1\\j\neq k}}^{t}\frac{x-x_j}{x_k-x_j}(\mathrm{mod}\ p)$

这里， $l_k(x_j)=\begin{cases}1 & 当\ k=j\ 时\\2 & 当\ k\neq j\ 时\end{cases}$

这里是因为 l_k 中包含为零的因子 $(x-x_j)/(x_k-x_j)$ 因子。而拉格朗日差值多项式

$$f(x)=\sum_{k=1}^{t}\lambda_k l_k(x)$$

当 $1\le j\le t$ 时，满足 $f(x_j)=\lambda_j$ 。

b)通过点（ x_1， λ_1 ），（ x_2， λ_2 ），…，（ x_t， λ_t ）重构 $t-1$ 阶的多项式 $s(x)$ ，这意味着已知 t 个 t 元一次方程 $\lambda_k=a_0+a_1x+a_2x+\cdots+a_{t-1}x^{t-1}(\bmod p)$ ， $1\le k\le t$ 。

其中（ x_i， λ_i ）已知，方程系数未知。那么可以重写上式如下：

$$\begin{pmatrix}1 & x_1 & \cdots & x_1^{t-1}\\ 1 & x_2 & \cdots & x_2^{t-1}\\ \vdots & \vdots & & \vdots\\ 1 & x_t & \cdots & x_t^{t-1}\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ \vdots\\ a_{t-1}\end{pmatrix}=\begin{pmatrix}y_1\\ y_2\\ \vdots\\ y_t\end{pmatrix}\bmod p$$

左边的 $t\times t$ 矩阵是一个范德蒙矩阵，它的行列式 $D=\prod_{s\ge m>n\ge 1}(x_m-x_n)$ 。因为 $x_1,x_2,\cdots,x_t$ 互不相等，所以 $D\ne 0$ 。由线性方程组的卡莱姆法则，知方程组有唯一解。又因为前面已经在证明多项式 $f(x)$ 是一个解，故而 $f(x)=s(x)$ 。证明完毕。

实质上，本方案的正确性是建立在 Shamir 门限方案正确性的基础上的。

4.2 抗攻击性

下面结合方案中可能遭受的攻击，分析方案的安全性。

a）攻击者试图通过（ x_i， p_{ij} ）得到（ x_i， p_{ij} ），从而恢复出秘密 k 。

分析：假设黑盒子的数据是无法破解的。如果攻击者只得到（ x_i， p_{ij} ），而无法解密黑盒子 $\Rightarrow$ 只得到子密钥而得不到特征值 $\Rightarrow$ 得不到 t 个方程组 $\Rightarrow$ 求不出 $f(x)$ $\Rightarrow$ 得不到密钥。因此，仅仅得到（ x_i， p_{ij} ）是无法破解密钥 k 的。

b）攻击者通过伪造 p_{ij}，分发给参与者错误的子密钥。

分析：同一秘密参与者分得的子密钥所对应的特征值是相同的，同一集合的参与者可以将子密钥在黑盒子中进行验证，如果所得到的特征值不相同，则说明该系统受到了攻击，进而可以进行责任追究，反之，则说明系统是安全的。此外，黑盒子的应用也是本方案的创新点。

4.3 完善性证明

1） $t-1$ 个参与者无法恢复密钥 k 。

证明 参与者必须通过 $t-1$ 个方程求解 t 个未知数，其中至少有 1 个自由变量，则能得到正确秘密的概率最多为 $1/q$ ，与穷举无异，所以无法恢复秘密。由此可证明本方案是一个完善的门限秘密共享方案。

2）信息率

由于 a_1， a_2，…， a_{t-1}，都是从 Z_q 中随机的取出的值，所以集合 $\{\lambda_i\}$ 和子密钥的概率分布都是均匀分布的。所以用上述方法构造出来的秘密共享方案的信息率为

$$\rho=\frac{H(k)}{\max_{i=1}^{n}H(\lambda_i)}=\frac{\log|H(k)|}{\max_{i=1}^{n}\log|H(\lambda_i)|}=\frac{\log|Z_q|}{\max_{i=1}^{n}\log|Z_q|}=1$$

通过以上证明，知本方案是完备的理想秘密共享方案。

5 方案的具体应用

为了说明方案的可操作性，给出以下例子。

例：设有 3 个集合 B_1、B_2 和 B_3 ，它们分别有 2、3 和 2 个秘密参与成员。试为这 7 个用户分配密钥，并分析重构密钥 k 的过程。

1）参数选取

秘密分发者随机选取一个 2（此时 t 为 3）次的多项式： $f(x)=3+2x+x^2 \bmod 17$ 。

2）秘密分发

取 $\lambda_1=f(x_1)=f(1)=6$ 、 $\lambda_2=f(x_2)=f(2)=11$ 、 $\lambda_3=f(x_3)=f(4)=10$ ，此时的对角矩阵为

$$\Lambda=\begin{pmatrix}6&0&0&0&0&0&0\\0&6&0&0&0&0&0\\0&0&11&0&0&0&0\\0&0&0&11&0&0&0\\0&0&0&0&11&0&0\\0&0&0&0&0&10&0\\0&0&0&0&0&0&10\end{pmatrix}$$

秘密分发者生成的随机对称矩阵 Λ ：

$$P=\begin{pmatrix}\frac{377}{482}&\frac{1077}{15347}&\frac{843}{1331}&\frac{331}{8051}&\frac{233}{9616}&\frac{3001}{4158}&\frac{349}{394}\\ \frac{1077}{15347}&\frac{651}{701}&\frac{419}{554}&\frac{488}{1293}&\frac{1469}{1761}&\frac{653}{951}&\frac{347}{625}\\ \frac{843}{1331}&\frac{419}{554}&\frac{1831}{2695}&\frac{2126}{4973}&\frac{289}{1774}&\frac{948}{1367}&\frac{853}{1643}\\ \frac{331}{8051}&\frac{488}{1293}&\frac{2126}{4973}&\frac{313}{431}&\frac{634}{6647}&\frac{802}{1785}&\frac{167}{171}\\ \frac{233}{9616}&\frac{1469}{1761}&\frac{289}{1774}&\frac{634}{6647}&\frac{1119}{2770}&\frac{805}{2878}&\frac{661}{2919}\\ \frac{3001}{4158}&\frac{653}{951}&\frac{948}{1367}&\frac{802}{1785}&\frac{805}{2878}&\frac{395}{742}&\frac{361}{1210}\\ \frac{349}{394}&\frac{347}{625}&\frac{853}{1643}&\frac{167}{171}&\frac{661}{2929}&\frac{361}{1210}&\frac{403}{2724}\end{pmatrix}$$

生成的矩阵 A ：

$$A=P^{-1}\Lambda P=\begin{pmatrix}\frac{2598}{449}&\frac{1777}{931}&-\frac{704}{395}&\frac{280}{17131}&\frac{1195}{514}&-\frac{1023}{454}&-\frac{3651}{1081}\\ \frac{332}{165}&\frac{5781}{367}&\frac{4259}{773}&\frac{478}{205}&\frac{3220}{671}&\frac{7694}{1381}&\frac{7479}{1295}\\ \frac{506}{223}&-\frac{432}{1331}&\frac{7487}{540}&\frac{4211}{4374}&\frac{4157}{2592}&\frac{3137}{794}&\frac{1168}{187}\\ \frac{9199}{3992}&-\frac{1629}{893}&\frac{284}{6857}&\frac{2907}{301}&-\frac{2446}{1033}&\frac{363}{1168}&\frac{709}{1138}\\ -\frac{2471}{473}&-\frac{2648}{389}&-\frac{2832}{319}&-\frac{48}{13}&\frac{1337}{274}&-\frac{1727}{195}&-\frac{2987}{329}\\ \frac{2397}{710}&-\frac{391}{63}&-\frac{4334}{867}&-\frac{657}{235}&-\frac{4271}{482}&\frac{2534}{465}&-\frac{373}{57}\\ -\frac{1525}{354}&\frac{1309}{422}&-\frac{1635}{9491}&\frac{793}{600}&\frac{2465}{652}&-\frac{470}{783}&\frac{3229}{336}\end{pmatrix}$$

其中： λ_1 对应的特征向量为

$$p_{11}=\begin{pmatrix}-\frac{268}{4401}&\frac{91}{244}&\frac{301}{738}&-\frac{108}{1555}&-\frac{1342}{2627}&-\frac{453}{700}&\frac{207}{2615}\end{pmatrix}^T$$ 和

$$p_{12}=\begin{pmatrix}\frac{449}{1356}&\frac{967}{3611}&\frac{650}{19559}&-\frac{773}{3057}&-\frac{15931}{61273}&-\frac{1021}{1421}&\frac{302}{773}\end{pmatrix}^T$$ ；

λ_2 对应的特征向量为：

$$p_{21}=\left(-\frac{194}{2291}\quad -\frac{494}{3159}\quad -\frac{1016}{1945}\quad \frac{323}{2066}\quad \frac{157}{2715}\quad \frac{258}{325}\quad -\frac{506}{2593}\right)^T、$$

$$p_{22}=\left(\frac{283}{594}\quad -\frac{793}{4033}\quad -\frac{878}{1607}\quad \frac{1423}{3801}\quad \frac{628}{1161}\quad -\frac{169}{6768}\quad -\frac{82}{3107}\right)^T 和$$

$$p_{23}=\left(-\frac{1841}{12482}\quad \frac{149}{2844}\quad -\frac{1001}{2271}\quad \frac{321}{1754}\quad -\frac{416}{1689}\quad \frac{475}{593}\quad -\frac{547}{2566}\right)^T；$$

λ_3 对应的特征向量为

$$p_{31}=\left(-\frac{887}{3204}\quad \frac{366}{1103}\quad \frac{414}{1349}\quad \frac{228}{2009}\quad -\frac{405}{749}\quad -\frac{691}{1397}\quad \frac{1145}{2784}\right)^T 和$$

$$p_{32}=\left(\frac{481}{978}\quad \frac{1091}{12978}\quad -\frac{613}{1507}\quad -\frac{379}{1165}\quad \frac{651}{1121}\quad -\frac{1099}{3121}\quad \frac{57}{419}\right)^T。$$

秘密分发者将这 7 个特征向量作为子密钥，即可得到 3 组子密钥：

第一组：k_{11} =（1，p_{11}），k_{12} =（1，p_{12}）；

第二组：k_{21} =（2，p_{21}），k_{22} =（2，p_{22}），k_{23} =（2，p_{23}）；

第三组：k_{31} =（4，p_{31}），k_{32} =（4，p_{32}）。将上述 3 组子密钥分别分发给 B_1、B_2 和 B_3 中的秘密参与成员。

3）秘密恢复

假设持有子密钥的 k_{11}，k_{21}，k_{31} 的 $1+1+1$ 个参与成员想要恢复密钥，他们首先需要将自己手中的子密钥输入黑盒中得到 $ch_1=\lambda_1=6$，$ch_2=\lambda_2=11$，$ch_3=\lambda_3=10$。

因为到场的人数为 3，则可以重构 $f(x)$。式子的三项分别为

$$\begin{aligned}&6\frac{(x-2)(x-4)}{(1-2)(1-4)}=6\frac{(x-2)(x-4)}{(-1)(-3)}\\&=6(x-2)(x-4)\bullet(3^{-1}\bmod 17)\\&=6(x-2)(x-4)\bullet 6=36(x-2)(x-4)\end{aligned}$$

$$\begin{aligned}&11\frac{(x-1)(x-4)}{(2-1)(2-4)}=\\&11\frac{(x-1)(x-4)}{-2}=11(x-1)(x-4)\bullet((-2)^{-1}\bmod 17)\\&=11(x-1)(x-4)\bullet 8=88(x-1)(x-4)\end{aligned}$$

$$\begin{aligned}&10\frac{(x-1)(x-2)}{(4-1)(4-2)}=10\frac{(x-1)(x-2)}{6}\\&=10(x-1)(x-2)\bullet(6^{-1}\bmod 17)\\&=10(x-1)(x-2)\bullet 3=30(x-1)(x-2)\end{aligned}$$

所以

$$\begin{aligned}&f(x)=[36(x-2)(x-4)+88(x-1)(x-4)\\&+30(x-1)(x-2)]\bmod 17\\&=(154x^2+746x+700)\bmod 17\\&=x^2+15x+3\end{aligned}$$

所以 $K=3$。从而获得共享密钥。

6　结束语

本文首次基于特殊对称矩阵的特征值提出了一种新的秘密共享方案。一个集合中多个参与者对应同一个特征值。1 个秘密被 t 个集合中的 n 个参与者所共享，只有所有集合的参与者都参与密钥恢复，才能恢复出密钥。同时，本方案利用黑盒子，实现子秘密的生成和主密钥的恢复，无论是在理论还是在工程应用方面都具有借鉴性意义。

参考文献：

[1] Shamir A. How to share a secret [J]. Comm ACM, 1979, 22 (11): 612-613.

[2] Blakley G R. Safeguarding cryptographic keys [C]// Proc of IEEE Computer Society, 1979: 313-317.

[3] Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure [J]. Electronics & Communications in Japan, 1989, 72 (9): 56-64.

[4] Laih C S, Harn L, Lee J Y, *et al.* Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space [C]// Advances in Cryptology. New YorkSpringer-Verlag, 1989: 286-298.

[5] Traverso G, Demirel D, Buchmann J. Dynamic and verifiable hierarchical secret sharing [C]// Proc of International Conference on Information Theoretic Security. Springe. 2016: 24-43.

[6] Zarepour-Ahmadabadi J, Shiri-Ahmadabadi M E, Miri A, *et al.* A new gradual secret sharing scheme with diverse access structure [J]. Wireless Personal Communications, 2018 (2): 1-16.

[7] Yang S, Wu H, Li J. Access structures of hyperelliptic secret sharing schemes [J]. Finite Fields & Their Applications, 2016, 37: 46-53.

[8] Binu V P, Sreekumar A. Secure and efficient secret sharing scheme with general access structures based on elliptic curve and pairing [J]. Wireless Personal Communications, 2017, 92 (4): 1531-1543.

[9] Jarecki S, Kiayias A, Krawczyk H. Round-optimal password-protected secret sharing and T-PAKE in the password-only model [C]// Advances in Cryptology – ASIACRYPT 2014. Berlin: Springer, 2014: 233-253.

[10] Pilaram H, Eghlidos T. An efficient lattice based multi-stage secret sharing scheme [J]. IEEE Trans on Dependable & Secure Computing, 2017, 14 (1): 2-8.

[11] Sarkar P, Nandi S, Chowdhury M U. Publicly verifiable secret sharing scheme in hierarchical settings using CLSC over IBC [C]// Proc of International Conference on Applications and Techniques in Cyber Security and Intelligence. 2017: 194-205.

[12] Wang N, Fu J, Zeng J. Verifiable secret sharing scheme without dealer based on vector space access structures over bilinear groups [J]. Electronics Letters, 2018, 54 (2): 77-79.

[13] 同济大学数学系编. 工程数学线性代数 [M]. 北京：高等教育出版社, 2014: 124-128. (School of Mathematic Sciences, Tongji University. Engineering mathematics, linear algebra [M]. Beijing: Higher Education Press. 2014: 124-128.)

[14] 曹尔强, 张沂, 曹晔, 潘继宏. “软件黑盒子”文件加锁和加密的一个方法 [J]. 长春邮电学院学报, 1991 (3): 11-14. (Cao Erqiang, Zhang Yi, Cao Ye, *et al.* A technique of locking a disk and secreting a whole disk [J]. Journal of Changchun Post & Telecommunication Institute, 1991 (3): 11-14.)

[15] 谷利泽, 郑世慧, 杨义先, 等. 现代密码学教程 [M]. 北京：北京邮电大学出版社, 2009: 338-341. (Gu Lize, Zheng Shihui, Yang Yixian, *et al.* Modern cryptography course [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2009: 338-341.)